МІЖНАРОДНИЙ ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ «ЄВРОПЕЙСЬКА ШКОЛА БІЗНЕСУ»

Кафедра менеджменту та економіки

УЗГОДЖУЮ
Директор Навчально-наукового інституту «Європейська школа бізнесу»
_____ О. Чатченко
"___" _____2021 р.

ЗАТВЕРДЖУЮ
Завідувач кафедри менеджменту та економіки
_____ Ю. Ремига
"12" 01 2021 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРБЕЗПЕКА

(шифр і назва навчальної дисципліни)

Рівень вищої освіти: Перший (бакалаврський) рівень

Ступінь вищої освіти: бакалавр

Галузь знань: 07 «Управління та адміністрування»

Спеціальність: 073 «Менеджмент»

Київ – 2021

РОЗРОБЛЕНО ТА ВНЕСЕНО:

Приватний заклад вищої освіти «Міжнародний європейський університет».

РОЗРОБНИК ПРОГРАМИ:

завідувач кафедри менеджменту та економіки,
кандидат економічних наук, доцент _____ Ю. Ремига

Робоча програма навчальної дисципліни обговорена та схвалена на засіданні кафедри менеджменту та економіки,
протокол №_1_ від «_12_» _____01_____ 2021 р.

Завідувач кафедри менеджменту та економіки _____ Ю. Ремига

Плановий термін між ревізіями – 1 рік
Контрольний примірник

ВСТУП

Програма вивчення навчальної дисципліни «Кібербезпека» складена відповідно до Стандарту вищої освіти України (далі – Стандарт) першого (бакалаврського) рівня галузі знань 07 «Управління та адміністрування» спеціальності 073 «Менеджмент».

Опис навчальної дисципліни (анотація). Дана навчальна дисципліна є напрямок, який пов'язаний з розробкою, реалізацією, впровадженням та управлінням комплексними програмно-технічними системами захисту інформації в установі (компанії, підприємстві). Крім того, цей напрямок також пов'язане зі створенням і аудитом комп'ютерних систем, що впливають на безпеку транспортних, енергетичних, медичних та інших комплексів.

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань 07 «УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ»</td><td colspan="2"><u>Вибіркова</u></td></tr>
<tr><td>Розділів – 2</td><td rowspan="10">Спеціальність:
073 «Менеджмент»</td><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових розділів – 2</td><td>3-й</td><td>3-й</td></tr>
<tr><td rowspan="8">Загальна кількість годин – 90</td><td colspan="2">Семестр</td></tr>
<tr><td>6-й</td><td>6-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>24 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>16 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>50 год.</td><td>84 год.</td></tr>
<tr><td>Тижневе навантаження: аудиторних – 2,5 самостійної роботи студента – 3</td><td>Освітній рівень:
Перший (бакалаврський) рівень</td><td colspan="2">Вид контролю:</td></tr>
<tr><td><u>залік</u></td><td><u>залік</u></td></tr>
</table>

Предметом вивчення навчальної дисципліни є розвиток безпечного, стабільного і надійного кіберпростору має полягати в тому числі і завдяки «підвищенню цифрової грамотності громадян та культури безпечного поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту». Велика кількість персональних даних потрапляє до комп'ютерних соцмереж. Важливо розуміти рівні захищеності власних даних, правила використання платіжних систем, наслідки, які можуть спричинити конфіденційні дані, що потрапили у відкритий доступ або у розпорядження кіберзлочинців.

Міждисциплінарні зв'язки: навчальна дисципліна «Кібербезпека» базується на знаннях таких дисциплін, як «Економічне планування та прогнозування», «Менеджмент», «Економічний аналіз» та взаємопов'язана з

дисциплінами «Аналіз господарської діяльності підприємств», «Логістика», «Організація підприємницької діяльності», «Операційний менеджмент», «Контролінг».

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1.1. **Метою** викладання навчальної дисципліни «Кібербезпека» є навчити студента основні концепції безпеки інформації, і дає змогу отримати навички, необхідні для моніторингу, виявлення, аналізу і нейтралізації загроз інформаційної безпеки.

1.2. Основними **завданнями** вивчення дисципліни «Кібербезпека» є:

– наданні студентам базових теоретичних знань у галузі інформаційної безпеки;

– наданні студентам базових знань щодо процесу створення безпечних інформаційних систем та процесів підтвердження їх відповідності;

– набутті студентами практичних навичок застосування сучасних технологій забезпечення інформаційної безпеки;

– вивченні основних принципів забезпечення інформаційної безпеки.

1.3. **Компетентності та результати навчання,** формуванню яких сприяє дисципліна (взаємозв'язок з нормативним змістом підготовки здобувачів вищої освіти, сформульованим у термінах результатів навчання у Стандарті).

Згідно з вимогами стандарту дисципліна забезпечує набуття студентами ***компетентностей*:**

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми, які характеризуються комплексністю і невизначеністю умов, у сфері менеджменту або у процесі навчання, що передбачає застосування теорій та методів соціальних та поведінкових наук.
Загальні компетентності	ЗК 4. Здатність застосовувати знання у практичних ситуаціях. ЗК 8. Навички використання інформаційних і комунікаційних технологій. ЗК 14. Здатність працювати у міжнародному контексті. ЗК 16. Здатність використовувати та дотримуватися національних та міжнародних стандартів, чинних правових норм у своїй професійній діяльності.
Спеціальні (фахові, предметні) компетентності	СК 6. Здатність діяти соціально відповідально і свідомо. СК 13. Розуміти принципи і норми права та використовувати їх у професійній діяльності. СК 16. Здатність розуміти та уміло використовувати математичні та числові методи, які часто використовуються для доцільності прийняття управлінських рішень, в тому числі, у розрізі міжнародної економічної діяльності.

Деталізація компетентностей відповідно до дескрипторів НРК у формі «Матриці компетентностей».

Матриця компетентностей

№	Компетентність	Знання	Уміння / навички	Комунікація	Автономія та відповідальність
Інтегральна компетентність					
1.	здатність розв'язувати складні спеціалізовані задачі та практичні проблеми, які характеризуються комплексністю і невизначеністю умов, у сфері менеджменту або у процесі навчання, що передбачає застосування теорій та методів соціальних та поведінкових наук.	Концептуальні наукові та практичні знання, критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання	донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації збір, інтерпретація та застосування даних; спілкування з професійних питань, у т.ч. іноземною мовою, усно та письмово	управління складною технічною або професійною діяльністю чи проектами; спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах; формування суджень, що враховують соціальні, наукові та етичні аспекти; організація та керівництво професійним розвитком осіб та груп; здатність продовжувати навчання із значним ступенем автономії
Загальні компетентності					
2.	Здатність застосовувати знання у практичних ситуаціях. Навички використання інформаційних і комунікаційних технологій. Здатність працювати у міжнародному контексті. Здатність використовувати та дотримуватися національних та міжнародних стандартів, чинних правових норм у своїй професійній діяльності.	Концептуальні наукові та практичні знання, критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання	донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації збір, інтерпретація та застосування даних; спілкування з професійних питань, у т.ч. іноземною мовою, усно та письмово	управління складною технічною або професійною діяльністю чи проектами; спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах; формування суджень, що враховують соціальні, наукові та етичні аспекти;

					організація та керівництво професійним розвитком осіб та груп; здатність продовжувати навчання із значним ступенем автономії
Спеціальні (фахові, предметні) компетентності					
3.	Здатність діяти соціально відповідально і свідомо. Розуміти принципи і норми права та використовувати їх у професійній діяльності. Здатність розуміти та уміло використовувати математичні та числові методи, які часто використовуються для доцільності прийняття управлінських рішень, в тому числі, у розрізі міжнародної економічної діяльності.	Концептуальні наукові та практичні знання, критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання	донесення до фахівців і нефахівців інформації, ідей, проблем, рішень, власного досвіду та аргументації збір, інтерпретація та застосування даних; спілкування з професійних питань, у т.ч. іноземною мовою, усно та письмово	управління складною технічною або професійною діяльністю чи проектами; спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах; формування суджень, що враховують соціальні, наукові та етичні аспекти; організація та керівництво професійним розвитком осіб та груп; здатність продовжувати навчання із значним ступенем автономії

Інтегративні кінцеві програмні результати навчання, формуванню яких сприяє навчальна дисципліна:

Програмні результати навчання	ПРН 1. Знати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства, верховенства права, прав і свобод людини і громадянина в Україні. ПРН 4. Демонструвати навички виявлення проблем та обґрунтування управлінських рішень. ПРН 6. Виявляти навички пошуку, збирання та аналізу інформації, розрахунку показників для обґрунтування управлінських рішень. ПРН 8. Застосовувати методи менеджменту для забезпечення ефективності діяльності організації. ПРН 11. Демонструвати навички аналізу ситуації та здійснення комунікації у різних сферах діяльності організації.

	ПРН 12. Оцінювати правові, соціальні та економічні наслідки функціонування організації. ПРН 20. Демонструвати навички використання інформаційних, комунікаційних та інноваційних технологій.

Результати навчання:
Після опанування дисципліни студент повинен
знати:

- концепцію та стандарти кібербезпеки;
- концепцію авторизації, аутентифікації та акаунтінгу ;
- концепцію віртуальних приватних мереж;
- безпеку на рівні комутації та маршрутизації;
- безпеку віртуальних локальних мереж;
- систему виявлення атак (вторгнень);
- систему запобігання вторгненням.

Уміти:

- захищати доступ до мережевого обладнання;
- виявляти сучасні загрози в мережі;
- налаштовувати системи система запобігання вторгненням;
- налаштовувати списки контролю доступу;
- налаштовувати зональний між мережевий екран;
- впроваджувати система виявлення атак (вторгнень);
- впроваджувати система запобігання вторгненням.

2. ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

На вивчення навчальної дисципліни «Кібербезпека» відводиться 90 години 3 кредити ЄКТС.

ЗМІСТОВИЙ РОЗДІЛ 1
СТАНДАРТИ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКИ

Тема 1. Теоретичні та методологічні основи захисту інформації.

Базові поняття у галузі інформаційної безпеки. Складові інформаційної безпеки. Характеристика інформації як предмета захисту. Інформація як об'єкт права власності. Сутність та цілі захисту інформації. Циклічна модель інформаційної безпеки. Потенційні загрози безпеки інформації та їх класифікація.

Тема 2. Структура законодавства в сфері захисту інформації.

Загальна характеристика законодавчих актів в сфері захисту інформації. Захист інформації як об'єкт адміністративно-правового регулювання. Система

органів регулювання технічного захисту інформації України. Взаємодія суб'єктів системи технічного захисту інформації.

Тема 3. Законодавче регулювання діяльності у сфері захисту інформації.

Напрями реалізації державної політики у сфері захисту інформації. Ліцензування господарської діяльності у галузі захисту інформації. Дозвільна система проведення робіт у галузі технічного захисту інформації.

Тема 4. Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.

Етапи життєвого циклу засобів захисту інформації та їх характеристика. Питання сертифікації продукції в сфері захисту інформації. Державна експертиза у сфері захисту інформації.

Тема 5. Порядок і правила захисту інформації в комп'ютерних системах.

Класифікація автоматизованих систем в НД ТЗІ. Моделі захисту інформації в автоматизованій системі. Модель порушника інформаційної безпеки. Порядок і правила захисту інформації в КС/АС. Забезпечення доступності й цілісності інформації в АС.

Тема 6. Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.

Предмет криптографії. Криптосистеми та загрози їх безпеки. Симетричні та асиметричні криптосистеми. Формування та перевіряння електронного цифрового підпису. Порядок забезпечення криптографічного захисту інформації.

Тема 7. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.

Провідні світові та національні органи зі стандартизації. Нормативне регулювання у сфері інформаційної безпеки в ЄС. Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки.

Тема 8. Стандарти інформаційної та кібернетичної безпеки.

Сімейство стандартів інформаційної та кібернетичної безпеки. Структура стандарту по кібербезпеці. Базові блоки стандарту ISO 27032. Заходи забезпечення кібербезпеки. Основи обміну інформацією та координації.

3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	Інд.	С. р.		л	п	лаб.	Інд.	С. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий розділ 1. Стандарти захисту інформації та кібербезпеки												
Тема 1. Теоретичні та методологічні основи захисту інформації.	11	4	1	-	-	6	12	2	-	-	-	10
Тема 2. Структура законодавства в сфері захисту інформації	10	2	2	-	-	6	11	-	1	-	-	10
Тема 3. Законодавче регулювання діяльності у сфері захисту інформації.	10	2	2	-	-	6	10	-	-	-	-	10
Тема 4. Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.	11	4	1	-	-	6	10	-	-	-	-	10
Тема 5. Порядок і правила захисту інформації в комп'ютерних системах.	10	2	2	-	-	6	10	-	-	-	-	10
Тема 6. Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.	12	4	2	-	-	6	10	-	-	-	-	10
Тема 7. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.	10	2	2	-	-	6	11	-	1	-	-	10
Тема 8. Стандарти інформаційної та кібернетичної безпеки.	14	4	2	-	-	6	12	2	-	-	-	10
Розрахункова робота	2	-	2	-	-	2	4	-	-	-	-	4
Разом за змістовим розділом 1	**90**	**24**	**16**	**-**	**-**	**50**	**90**	**4**	**2**	**-**	**-**	**84**
Усього годин	**90**	**24**	**16**	**-**	**-**	**50**	**90**	**4**	**2**	**-**	**-**	**84**

4. ТЕМИ ЛЕКЦІЙ

№ з/п	Назва теми	Кількість годин
1.	Теоретичні та методологічні основи захисту інформації.	4
2.	Структура законодавства в сфері захисту інформації	2
3.	Законодавче регулювання діяльності у сфері захисту інформації.	2
4.	Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.	4
5.	Порядок і правила захисту інформації в комп'ютерних системах	2
6.	Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.	4

7.	Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.	2
8.	Стандарти інформаційної та кібернетичної безпеки.	4
Разом:		**24**

5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ

Програмою навчальної дисципліни семінарські заняття не передбачені.

6. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1.	Теоретичні та методологічні основи захисту інформації.	1
2.	Структура законодавства в сфері захисту інформації	2
3.	Законодавче регулювання діяльності у сфері захисту інформації.	2
4.	Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.	1
5.	Порядок і правила захисту інформації в комп'ютерних системах	2
6.	Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.	2
7.	Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.	2
8.	Стандарти інформаційної та кібернетичної безпеки.	2
9.	*Розрахункова робота*	2
Разом:		**16**

7. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

Програмою навчальної дисципліни лабораторні заняття не передбачені.

8. САМОСТІЙНА РОБОТА

№ з/п	Назва теми	Кількість годин
1.	Теоретичні та методологічні основи захисту інформації.	6
2.	Структура законодавства в сфері захисту інформації	6
3.	Законодавче регулювання діяльності у сфері захисту інформації.	6
4.	Процедури забезпечення необхідних характеристик та якості засобів захисту інформації.	6
5.	Порядок і правила захисту інформації в комп'ютерних системах	6
6.	Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.	6
7.	Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.	6
8.	Стандарти інформаційної та кібернетичної безпеки.	6
9.	*Розрахункова робота*	2
Разом:		**50**

9. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Розрахункова робота

Завдання 1. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки.

1.1. Провідні світові та національні органи зі стандартизації.

1.2. Нормативне регулювання у сфері інформаційної безпеки в ЄС.

1.3. Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки.

Завдання 2. Стандарти інформаційної та кібернетичної безпеки.

2.1. Сімейство стандартів інформаційної та кібернетичної безпеки.

2.2. Структура стандарту по кібербезпеці.

2.3. Базові блоки стандарту ISO 27032.

2.4. Заходи забезпечення кібербезпеки.

2.5. Основи обміну інформацією та координації.

Завдання 3. Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку.

3.1. Предмет криптографії.

3.2. Криптосистеми та загрози їх безпеки.

3.3. Симетричні та асиметричні криптосистеми.

3.4. Формування та перевіряння електронного цифрового підпису.

3.5. Порядок забезпечення криптографічного захисту інформації.

Завдання 4. Управління ризиками.

4.1. Модель безпеки з повним перекриттям

4.2. Основні принципи побудови концепції ІБ

4.3. Основні вимоги міжнародного стандарту ISO 15408.

4.4. Методика визначення потенціалу нападу при оцінці стійкості функцій безпеки.

4.5. Профіль захисту ІБ.

Завдання 5. Методологія оцінки ризиками.

5.1. Основні принципи методології оцінки.

5.2. Основні принципи побудови концепції ІБ.

5.3. Методики побудови систем захисту інформації, що включають етап аналізу ризиків.

5.4. Методика "Facilitated Risk Analysis Process (FRAP)".

5.5. Методика оцінка серйозності мережевої атаки, яка використовується SANS / GIAC.

10. ТЕМИ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем для самостійної роботи студентів:

1. Складові інформаційної безпеки.
2. Аналіз концепції інформаційної безпеки України.
3. Дозвільна система проведення робіт у галузі технічного захисту інформації.
4. Аналіз пошукових систем для конкурентної розвідки.
5. Забезпечення доступності й цілісності інформації в АС.
6. Порядок забезпечення криптографічного захисту інформації.
7. Циклічна модель інформаційної безпеки. Потенційні загрози безпеки інформації та їх класифікація.
8. Взаємодія суб'єктів системи технічного захисту інформації.
9. Ліцензування господарської діяльності у галузі захисту інформації.
10. Сертифікація продукції в сфері захисту інформації.
11. Модель порушника інформаційної безпеки.
12. Криптосистеми та загрози їх безпеки.

11. МЕТОДИ НАВЧАННЯ

При викладанні навчальної дисципліни «Кібербезпека» застосовуються інформаційні та практичні методи навчання: класичні лекції, лекції-дискусії, практичні заняття, консультації з виконання самостійної та індивідуальної роботи студентів, а також виконання рефератів, підготовка коротких повідомлень на основі додаткової літератури курсу, письмові завдання при проведенні контрольних робіт.

Методи навчально-пізнавальної діяльності: пояснювально-ілюстративний метод, репродуктивний метод, метод проблемного викладу, частково-пошуковий або евристичний метод, дослідницький метод.

Методи стимулювання й мотивації навчально-пізнавальної діяльності: індуктивні і дедуктивні методи навчання, методи стимулювання і мотивації навчання.

12. МЕТОДИ КОНТРОЛЮ

Відповідно до плану вивчення дисципліни «Кібербезпека» передбачається проведення поточного та підсумкового контролю:

– поточний контроль передбачає проведення опитування під час практичних занять;

– контроль виконання всіх видів робіт;

– підсумковий контроль реалізується у вигляді заліку.

Методи контролю:

1. Оцінювання знань студента під час практичних занять.
2. Виконання завдань для самостійної роботи.
4. Проведення проміжних тестів.
5. Проведення поточного контролю.

6. Проведення підсумкового заліку.

13. ФОРМА ПІДСУМКОВОГО КОНТРОЛЮ УСПІШНОСТІ НАВЧАННЯ

Формою підсумкового контролю є **залік**, який складається очно в період призначений деканатом або за індивідуальним графіком, який затверджується навчальним планом. Основною формою підсумкового контролю є тестування, робота над практичним завданням та співбесіда.

14. СХЕМА НАРАХУВАННЯ ТА РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ

Оцінювання окремих видів виконаної студентом навчальної роботи з дисципліни «Кібербезпека» здійснюється в балах відповідно до табл.14.1. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку.

Таблиця 14.1

Розподіл балів оцінювання успішності студентів з навчальної дисципліни «Кібербезпека»

Розділ I Поточне тестування та самостійна робота									Розділ II Підсумковий контроль	Всього
Змістовий розділ 1										
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	РР		
5	5	5	5	5	10	5	10	10	40	100

**Т1, Т2, ..., Т8 – теми занять*

***Розрахункова робота*

Поточне оцінювання знань студентів проводиться протягом семестру у наступних формах: усного опитування студентів на практичних заняттях та оцінки рівня їх знань; перевірки правильності розв'язання практичних задач; експрес-опитування (в усній чи письмовій формі).

Загальна оцінка знань студентів за поточним контролем

Результати поточного контролю знань студентів в цілому (за усіма формами робіт) оцінюються в діапазоні від **0** до **60** балів. Студент допускається до підсумкового контролю за умови виконання вимог навчальної програми та у разі, якщо за поточну навчальну діяльність він набрав не менше **36** балів.

Підсумкове оцінювання знань студентів

Підсумкове оцінювання знань студентів проводиться у формі **заліку**.

Критерії оцінювання знань під час заліку.

Максимальна кількість балів, яку можна отримати на іспиті складає **40** балів (див. табл. 14.2).

Під час оцінювання відповіді на окреме питання додатково враховуються допущені недоліки та помилки, якими вважаються: неохайне оформлення

роботи (не загальноприйняті скорочення, незрозумілий почерк, використання олівців замість чітких чорнил) (мінус **2** бали); неточності в назвах окремих економічних категорій та понять (мінус **4** бали).

Таблиця 14.2

Розподіл балів оцінювання при підсумковому контролі з навчальної дисципліни «Кібербезпека»

Оцінка в балах за поточне оцінювання	Оцінка в балах за підсумкове оцінювання	Оцінка за національною шкалою
54-60	36-40	Відмінно
45-53	30-35	Добре
36-44	24-29	Задовільно
менше 36	менше 24	Незадовільно

Критерії оцінювання відповіді на теоретичні питання білету:

1. Повна відповідь на питання, яка оцінюється ***«відмінно»***, повинна відповідати таким вимогам:

– розгорнутий, вичерпний виклад змісту даної у питанні проблеми;

– повний перелік необхідних для розкриття змісту питання економічних категорій та законів;

– здатність здійснювати порівняльний аналіз різних теорій, концепцій, підходів та самостійно робити логічні висновки й узагальнення;

– уміння користуватись методами наукового аналізу економічних явищ, процесів і характеризувати їхні риси та форми виявлення;

– демонстрація здатності висловлення та аргументування власного ставлення до альтернативних поглядів на дане питання;

– використання актуальних фактичних та статистичних даних, знань дат та історичних періодів, які підтверджують тези відповіді на питання.

2. Відповідь на питання оцінюється ***«добре»***, якщо:

– відносно відповіді на найвищий бал не зроблено розкриття хоча б одного з пунктів, вказаних вище (якщо він явно потрібний для вичерпного розкриття питання) або, якщо:

– при розкритті змісту питання в цілому правильно за зазначеними вимогами зроблені окремі помилки під час: використання цифрового матеріалу.

3. Відповідь на питання оцінюється ***«задовільно»***, якщо:

– відносно відповіді на найвищий бал не зроблено розкриття чотирьох чи більше пунктів, зазначених у вимогах до нього (якщо вони явно потрібні для вичерпного розкриття питання);

– одночасно присутні чотири чи більше типів недоліків, які окремо характеризують критерій оцінки питання;

– висновки, зроблені під час відповіді, не відповідають правильним чи загально визначеним при відсутності доказів супротивного аргументами, зазначеними у відповіді;

– характер відповіді дає підставу стверджувати, що особа, яка складає іспит, не зовсім правильно зрозуміла зміст питання чи не знає правильної

відповіді і тому не відповіла на нього по суті, допустивши грубі помилки у змісті відповіді.

З урахуванням вищевикладеного результати іспиту оцінюються в діапазоні від **0** до **40** балів для студентів. При цьому, якщо відповіді студента на екзамені оцінені менше ніж на 30%, він отримує незадовільну оцінку за результатами іспиту та незадовільну загальну підсумкову оцінку. Загальна підсумкова оцінка з дисципліни складається з суми балів за результати поточного контролю знань та за виконання завдань, що виносяться на залік.

Загальна підсумкова оцінка не може перевищувати **100 балів**. Загальна підсумкова оцінка в балах, за національною шкалою та за шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента (див. табл. 14.3).

Таблиця 14.3

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
66-73	D	задовільно	
60-65	E		
30-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-29	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

15. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

- робоча навчальна програма дисципліни;
- плани лекцій, практичних занять та самостійної роботи студентів;
- тези лекцій з дисципліни;
- методичні рекомендації та розробки для викладача;
- методичні вказівки до практичних занять для студентів;
- методичні матеріали, що забезпечують самостійну роботу студентів;
- тестові та контрольні завдання до практичних занять;
- перелік питань та завдань для поточного і проміжного контролю знань з дисципліни;
- перелік питань до заліку, завдання для перевірки практичних навичок під час заліку.

16. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна (базова):

1. Гулак Г.М., Гринь А.К., Мельник С.В. Методологія захисту інформації: навчально-методичний посібник. – К.: Видавництво НА СБ України, 2015. – 251 с.

2. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432 с.

3. Цимбалюк В.С. Інформаційне право (теорія і практика). Монографія. – К.: 2009. - 364 с.

4. Кобозева А.А., Мачалін І.О., Хорошко В.О., Аналіз захищеності інформаційних систем. Підручник. – К.: вид. ДУІКТ, 2010. - 316 с.

5. Андрєєв В.І., Хорошко В.О., Чередніченко В.С., Шелест М.Є., Основи інформаційної безпеки. Підручник. – К.: вид. ДУІКТ, 2009. –292 с.

6. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

7. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки. /Невойт Я.В., Єрмошин В.В.// Монографія. – К: ДУТ, 2015. – 124 с.

8. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. /В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко/ –К.:ДУТ, 2015. – 345 с.

9. Богуш В.М., Довидьков О.А., Кривуца В.Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

Допоміжна:

1. Постанова Кабінету Міністрів України від 18.05.2011 року №517 Про затвердження переліку послуг у галузі технічного захисту інформації, господарська діяльність щодо надання яких підлягає ліцензуванню.

2. Постанова Кабінету Міністрів України від 25.05.2011 року №543 Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню.

3. Бекірова Е. Правова природа інституту ліцензування певних видів господарської діяльності // Підприємництво, господарство і право. – 2007, №10, С. 95-97.

4. Господарський кодекс України: Коментар. – Х.: "Одіссей", 2004. – 848 с.

17. ІНФОРМАЦІЙНІ РЕСУРСИ:

1. Верховна Рада України. Законодавство України // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/

2. Державна служба спеціального зв'язку та захисту інформації // [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.

3. CERT-UA // [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/